Simbian®

Simbian AI SOC Agent

In an AI SOC (AI-powered Security Operations Center) autonomous AI systems assist human analysts by triaging alerts, correlating signals, running investigations, and even executing responses. Instead of drowning in noise, your team sees fewer, higher-quality, risk-prioritized incidents and spends most of its time on strategic defense and threat hunting.

A New Class of Security

Simbian's AI SOC Agent **autonomously triages, investigates, and responds** to every alert in your system, combinig the best of Simbian's knowledge base with your business know-how.

- **Unlike SOARs,** there is no need to build and maintain play-books. The SOC Agent Investigates every alert with AI, even new and unknown threats.
- **Unlike Copilots,** the SOC Agent works autonomously, 24/7.
- **Unlike XDRs,** the SOC Agent investigates using data from across your entire environment, using Simbian's extensive ecosystem of 70+ integrations, for higher accuracy.
- **Unlike other emerging AI SOC solutions** Simbian's SOC Agent is complemented by a Threat Intel Agent to Ingest and Action Threat Intel, and a Threat Hunt Agent that hunts your entire environment based on threat hypotheses. These Agents work together to make SOC investigations much richer than standalone AI SOC solutions.

90%
Alerts resolved automatically

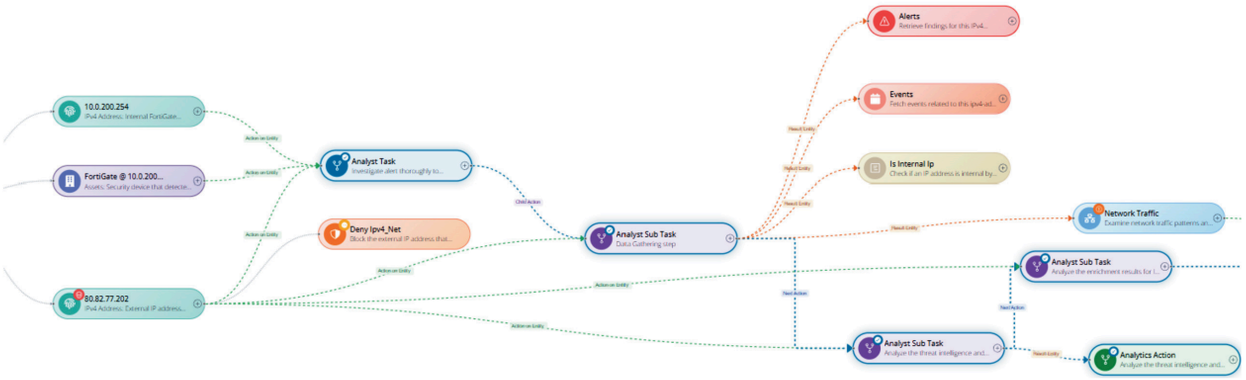
5x
Cost savings

9x
Faster Mean Time to Contain(MTTC)

0
Playbooks needed

24/7
Coverage

+1 650-695-0740 sales@simbian.ai www.simbian.ai



The SOC Agent uses a threat hunt methodology to deeply investigate every alert, correlate other events in the environment, and stitch together the big picture.

WHAT WE DO

Your SOC on Autopilot

Automated Response

The AI SOC Agent conducts a thorough investigation of an alert, collecting data from all available sources to determine whether it is a false or true positive. Based on the level of autonomy granted, the agent provides recommendations to the analyst for further action and can also autonomously take measures to contain threats.

Transparent reasoning

The AI SOC Agent clarifies its reasoning and verdict so that analysts can comprehend and validate its findings. The steps are summarised in simple language, allowing even non-analysts to understand and contribute.

New Alert? No Problem

If a novel attack is discovered, Simbian's AI SOC Agent acts immediately without waiting for your instructions. It conducts an initial assessment by gathering evidence from all available data sources across your entire ecosystem and provides a verdict just like it does with any other alert. This means no extensive playbooks are required, and there is no prolonged meantime to respond (MTTR) for new alerts.

Reporting and Documentation

The era of relying on manual playbooks is over; putting us at risk of breaches in case of a novel alert. With each verdict, reasoning, and action, the AI SOC Agent automatically writes the following steps and documentation directly into your SIEM or Case Management tool. All knowledge is added to the Context Lake™ for any future actions. With extensive evidence, reasoning, confidence ratings, and investigation graphs, analysts can follow the complete methodology, diving deeper or cross-questioning the agent whenever they wish.

HOW WE DO

The Simbian Way

Complete Alert Automation

As soon as an alert is raised by your detection tool (SIEM/SOAR/XDR), Simbian's AI SOC Agent is the first line of response. It gathers evidence from all available points within your ecosystem and, after analysis, provides a True/False Positive verdict. The process doesn't stop there; depending on the level of autonomy granted, the agent can take containment actions—such as isolating an endpoint—or provide a list of recommended actions for the analyst to consider. Each action taken by the agent can be thoroughly investigated, rechecked, and discussed with the agent itself, allowing for feedback and collaboration.

Context Lake™

What happens when your best analyst leaves? What happens to documentation when it's done unsystematically? With Simbian, there's nothing to worry about. During deployment, you can feed all your context and tribal knowledge into the system. With every action and interaction with the platform, our proprietary Context Lake is populated. As more threats and alerts are analyzed, more context is generated, allowing the agent to continuously improve.

Multi-Agent Architecture

At Simbian, we understand that security is not one-dimensional. Our platform includes agents across various domains such as Security Operations Center (SOC), Threat Hunting, Vulnerability management, Penetration Testing, and Governance, Risk, and Compliance (GRC). All agents continuously learn from each other to improve outcomes By partnering with Simbian, there is a cohesiveness amongst all agents. Learning constantly from each other and ensuring that your organization is protected across all domains. While enriching the Context Lake so organisational learnings are not lost.

Seamless and Rapid Deployment

The system functions through API-level integrations with EDR, SIEM, NDR, cloud, and identity providers—eliminating the need for PowerShell and endpoint agents. One unified agent synthesizes data across all connected tools and environments, providing greater context for more insightful analysis. Available as either a SaaS or on-premises solution, it can be deployed in just a few hours with minimal configuration required.

+1 650-695-0740 sales@simbian.ai www.simbian.ai